Ilyesse El Adaoui

Travail à Faire

-Mission 1 Informer les utilisateurs sur les risques et promouvoir les bons usages à adopter.

1. Identifiez les situations qui peuvent constituer un risque pour le SI de la MSAP.
   >Fiche savoirs technologiques 4
   > Document 1,2,3

Le mot de passe utilisé par les prestataires d'Enedis a une sécurité faible. En effet, une suite de chiffres est facilement trouvable par un ordinateur. Utiliser ses appareils personnels pour utiliser le serveur d'une entreprise est très dangereux. En effet, les particuliers ne sont pas tous sensibilisés à la protection de leur données ou à la protection de leur appareil personnel. Ce sont donc des cibles faciles à attaquer pour les pirates. Cela rend le SI de l'entreprise très vulnérable.

2. Précisez les bonnes pratiques à adopter par les utilisateurs du télécentre.
   >Fiche savoirs technologiques 4
   >Document 5 et 6

Les employés du télécentre doivent tester la sécurité de leur mot de passe sur le site How secure is my password. Ils doivent faire en sorte que leur mot de passe est une sécurité assez haute pour tenir 7 mois. Les ordinateurs des employés doivent être munis d'alerte de sécurité, ils doivent tous impérativement bénéficier de pare-feu et en aucun cas accepter des fichiers ou des logiciels dont le créateur n'est pas connu ou qui ne fait pas partie du serveur local.

3. Proposer des solutions pour limiter les risques de l'utilisation d'une messagerie.
   >Fiche savoirs technologiques 4
   >Document 7

Une messagerie professionnelle ne doit en aucun cas être communiquer ou utiliser à des fins commerciales. En effet, car sinon elle sera surement vendu à des personnes malveillantes qui essaieront de piéger les employés avec des mails de type phishing.

4. Rédiger la liste des points clés qui devront y figurer.
   >Fiche savoirs CEJMA 6
   >Document 8

Introduction

Cette charte a pour vocation de présenter les bonnes pratiques à adopter au sein du système d'information de la MSAP et , plus particulièrement, au niveau du télécentre. Elle stipule les droits et devoirs de chaque utilisateur.

1. **Ressources mises à disposition**

Chaque utilisateur peut avoir accès à un espace de travail privatif ou collectif, avec une connexion internet, un environnement bureautique Windows, un espace de reprographie et enfin une salle de visioconférence et de réunion. Un espace de stockage privatif est proposé sur le serveur de fichier de la MSAP.

2. **Les règles de sécurité en vigueur**

a. **Authentification sur les postes de travail**

Chaque utilisateur se voit attribuer un identifiant qui lui permettra de définir son mot de passe. L'identifiant est nominatif et ne peut être partagé avec un autre utilisateur. Le mot de passe est strictement confidentiel, le propriétaire est responsable de l'utilisation qui en est faite et s'engage à ne pas le communiquer à un tiers.

b. **Configuration des environnements de travail.**

La configuration des postes de travail fournie dans les différents espaces de travail permet d'assurer la sécurité des utilisateurs et de leurs données. Il ne faut pas intervenir sur l'installation automatique des correctifs.

c. **Environnement internet**

La connexion à certains sites pourrait fragiliser la sécurité du SI de la MSAP. Il faut donc être particulièrement vigilant dans la gestion de sa boîte de courriels professionnelle.

3. Conditions particulières liées à l'utilisation des outils nomades

L'utilisation des supports numériques personnels est autorisée. Cependant, leur configuration doit assurer la sécurité du SI de la MSAP. Ces supports ne doivent être utilisés que dans le cadre professionnel. Les téléchargements illicites sont interdits.

Je soussigné, ……., utilisateur des ressources numériques proposées par la MSAP de la commune de Marut, certifie avoir pris connaissance de la charte des bons usages de l'utilisation des SI de la MSAP, des droits et obligations qui en découlent et atteste que je suivais les instructions précisées dans celle-ci.

Date:
Signature

Bonjour Monsieur,
Dans votre charte informatique de la MSAP, on retrouve bien les objectifs (usages des ressources numériques, etc), les objets et portées de votre charte même si elle reste incomplète (pas de longueur de mot de passe définie, etc), nous avons aussi les usages reportés dans votre chartes même si elle aussi est incomplète car elle ne répond pas à la question des besoins auquel le SI doit répondre. Les devoirs des utilisateurs sont bien spécifiés.
En revanche , les éléments manquant dans votre charte sont les éléments suivants , les définitions claires et précises de certains termes comme l'authentification, les mesures de contrôles, les sanctions pour le non- respect des règles du SI de la MSAP et l'opposabilité de la charte.

Une fois ces éléments complétés dans votre charte, vous aurez de quoi sensibiliser vos employés à l'usage de votre SI.

Cordialement.